

DDWRT VLAN's revisited

(having fun with VAP's, WAP's and VLAN's

Introduction

When the VLAN world was simple and straightforward (at least for Broadcom) I already did a write up how to use [VAP's, WAP's and VLAN's](#) but that is now outdated since the introduction of swconfig for Broadcom, so a new write up.
AS I am still learning and have to discover a lot this is a WIP and no definitive answer so please share your results/answers/thoughts/corrections.

Note:
When creating bridges you have to be extremely patient, add a bridge, Apply and wait two minutes before creating another bridge. After you have created all bridges Reboot the router
Then Assign to Bridge, Add and Assign, then Apply and wait two minutes after assignment then assign the next interface to a bridge. In the end Reboot again. If you are not patient the bridge index becomes corrupt and all assignments revert to none

index

Introduction	1
Setup	1
Main router R7800	1
Screenshots of Main router (R7800).....	2
VLAN's and R7800	6
Secondary router R7000	7
Screenshots of WAP setup.....	9
Isolating subnets/bridges.....	15
Main router R7800.....	15
To research.....	15

Setup

Before setting this up both routers were reset to defaults

Main router R7800

Netgear R7800 running build 49626
Setup: Gateway, IP address 192.168.5.1


The router has two bridges which have their own IPAddresses/subnet
br1 is associated with VLAN 3
One trunk port to the WAP with VLAN1, VLAN3 and VLAN4 all tagged
One port (swconfig port 2 = port 3 on the router) on VLAN 3 (br1)
One VAP associated with br2 (VLAN 4)

Screenshots of Main router (R7800)

WAN Connection Type

Connection Type	Automatic Configuration - DHCP ▾
Ignore WAN DNS	<input checked="" type="checkbox"/>
Use VLAN Priority	<input type="checkbox"/>

Optional Settings

Router Name	R7800-2 
Hostname	<input type="text"/>
Domain Name	<input type="text"/>
MTU	Auto ▾ 1500
Shortcut Forwarding Engine	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Network Setup

Router IP

Local IP Address	192 · 168 · 5 · 1 / 24
Gateway	0 · 0 · 0 · 0
Local DNS	0 · 0 · 0 · 0

Dynamic Host Configuration Protocol (DHCP)

DHCP Type	DHCP Server ▾
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192 · 168 · 5 · 64
Maximum DHCP Users	190
Lease Expiration	1440 min
Static DNS 1	9 · 9 · 9 · 9
Static DNS 2	1 · 0 · 0 · 1
Static DNS 3	0 · 0 · 0 · 0
WINS	0 · 0 · 0 · 0
Use dnsmasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>
Recursive DNS Resolving (Unbound)	<input type="checkbox"/>

Create a Bridge

Name	STP	IGMP Snooping	Prio	Forward Delay	Max Age	MTU	Root MAC	Action
br0	Off ▾	Off ▾	32768 ▾	15	20	1500	BC:A5:11:3E:71:F1	⊖
br1	STP ▾	Off ▾	32768 ▾	15	20	1500	BC:A5:11:3E:71:F1	⊖
br2	STP ▾	Off ▾	32768 ▾	15	20	1500	BC:A5:11:3E:71:F1	⊖

Add

Assign to Bridge

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	Action
br1 ▾	wlan0.1 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖
br1 ▾	vlan3 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖
br2 ▾	vlan4 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖

Add

Current Bridging Table

Bridge Name	STP	Interface
br0	no	eth1 wlan0 wlan1
br1	yes	vlan3 wlan0.1
br2	yes	vlan4

Port Setup

WAN Port Assignment

eth0 ▼

Network Configuration eth1

MAC Address BC:A5:11:3E:71:F1

Label

TX Queue Length 1000

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration eth1.3

MAC Address BC:A5:11:3E:71:F1

Label

TX Queue Length 1000

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration eth1.4

MAC Address BC:A5:11:3E:71:F1

Label

TX Queue Length 1000

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration wlan0

MAC Address BC:A5:11:3E:71:F3

Label

TX Queue Length 1000

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration wlan0.1

MAC Address BE:A5:11:3E:71:F3

Label

TX Queue Length 1000

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration wlan1

MAC Address

BC:A5:11:3E:71:F4

Label

TX Queue Length

1000

Multicast to Unicast

☐ Enable

☒ Disable

Bridge Assignment

☒ Default

☐ Unbridged

Network Configuration br1

Label

TX Queue Length

1000

MTU

1500

Multicast Forwarding

☐ Enable

☒ Disable

Masquerade / NAT

☒ Enable

☐ Disable

Filter WAN NAT Redirection

☐ Enable

☒ Disable

Net Isolation

☐ Enable

☒ Disable

Forced DNS Redirection

☐ Enable

☒ Disable

IP Address

192

.

168

.

53

.

1

/

24

L2Mesh Enable

☐

L2Mesh Bridge

br0

▼

Network Configuration br2

Label

TX Queue Length

1000

MTU

1500

Multicast Forwarding

☐ Enable

☒ Disable

Masquerade / NAT

☒ Enable

☐ Disable

Filter WAN NAT Redirection

☐ Enable

☒ Disable

Net Isolation

☐ Enable

☒ Disable

Forced DNS Redirection

☐ Enable

☒ Disable

IP Address

192

.

168

.

54

.

1

/

24

L2Mesh Enable

☐

L2Mesh Bridge

br0

▼

DHCPD

Multiple DHCP Servers

IP Address	Interface	Enable	Start	Max	Lease time	Action
192.168.53.1/24	<div>br1</div> ▼	<div>On</div> ▼	<div>100</div>	<div>50</div>	<div>1440</div> min	⊖
192.168.54.1/24	<div>br2</div> ▼	<div>On</div> ▼	<div>100</div>	<div>50</div>	<div>1440</div> min	⊖

Add

VLAN's and R7800

On modern builds you can use the GUI just fine see ho1Aetoo,s excellent thread for routers with 2 CPU ports (e.g. R7800): <https://forum.dd-wrt.com/phpBB2/viewtopic.php?t=334342>

VLAN threads can be found as stickies in the Advanced Networking forum.

The old and now obsolete manual way is described below but it still works as the underlying technology is still swconfig.

I have added the script below to Startup (Administration/Commands Save as Startup).

Note: in swconfig the switch ports 1-4 are reversed so 1=4 and 2=3

```
## to enable VLANs
swconfig dev switch0 set enable_vlan 1
## tag VLAN 1 on the trunk port 3 which is actually port 2 on the router, this is
necessary
## as the WAP also has VLAN 1 1 tagged on the trunk port (the GUI of the R7000 allows
only all tagged)
swconfig dev switch0 vlan 1 set ports "1 4 3t 6"
swconfig dev switch0 vlan 3 set ports "3t 6t"
## set port 3 (which is port 2 on the router) to VLAN 3 and also the trunk port
swconfig dev switch0 vlan 4 set ports "2 3t 6t"
swconfig dev switch0 set apply

# if you use this then you can address eth1.3 as vlan3 see:
https://ixnfo.com/en/configuring-vlans-in-ubuntu.html
vconfig set_name_type VLAN_PLUS_VID_NO_PAD

vconfig add eth1 3
## you can also use the GUI to add vlan 3 to br1 for better overview
brctl addif br1 vlan3
#ifconfig vlan3 down # not necessary
ifconfig vlan3 up

# for use if VLAN_PLUS_VID_NO_PAD is NOT used
#brctl addif br1 eth1.3
#ifconfig eth1.3 down # not necessary
#ifconfig eth1.3 up

vconfig add eth1 4
## you can also use the GUI to add vlan 4 to br1 for better overview
brctl addif br2 vlan4
#ifconfig vlan4 down # not necessary
ifconfig vlan4 up

# for use if VLAN_PLUS_VID_NO_PAD is NOT used
#brctl addif br2 eth1.4
#ifconfig eth1.4 down # not necessary
#ifconfig eth1.4 up
```

Secondary router R7000

Netgear R7000, running Community build 52369 (the community build is home made with the community build system and has some extra software which is not important for this paper)

Setup: Wireless Access Point (WAP).

Note you need at least build 52369 as that one has the new and improved Switch config tab with CPU port.

For some more VLAN examples for routers with one CPU port (as the R7000 and most other routers) see ho1Aetoo 's excellent thread: <https://forum.dd-wrt.com/phpBB2/viewtopic.php?t=335568>

VLAN threads can be found as stickies in the Advanced Networking forum.

I deviate from [the wiki](#) in setting up a WAP and think that the wiki should be updated but that is just my personal opinion.

Note: for Best throughput enable CTF.

A Wireless Access Point (WAP) is secondary router connected wired LAN<>LAN on the same subnet as the primary router:

- On Basic Setup page:
 - WAN disabled
 - DHCP server Disabled (=off and NOT set as Forwarder!)
 - Local IP address in subnet of primary router but outside DHCP scope, make sure the used IP address is unique on your network you cannot have duplicates.
You can run udhcpd to give the WAP a static lease but because you can it doesn't mean you should ;)
 - Gateway **and** Local DNS pointing to primary router
- Keep DNSMasq enabled (both on Basic Setup page and Services page)
- On Setup > Advanced Routing, keep Operating mode in the default **Gateway** (the wiki says Router mode but do not do that, either it does not matter (this case) or break things)
- On Security > Firewall keep the **SPI Firewall enabled**, although you do not want a firewall it will be automatically disabled as there is no WAN so no need to change this setting from default.
- Connect LAN <> LAN (**do not use the WAN port** unless you really need that extra port, for most routers traffic still must use the CPU so performance is lacklustre and there are some routers where the WAN port is not added to br0 so the WAN port could be non-functional on some routers).

If you have unbridged VAP's or other applications running on your router you have to add the following rule to the firewall in order to get internet access from the VAP's etc.

In the web-interface of the router (**the WAP**): Administration/Commands save Firewall:

#Always necessary (alternatively set static route on main router and NAT traffic out via the WAN):

```
iptables -t nat -I POSTROUTING -o br0 -j SNAT --to $(nvram get lan_ipaddr)
```

Builds past 56490 need also to add the following rule to the firewall (see: <https://forum.dd-wrt.com/phpBB2/viewtopic.php?p=1303297>):

```
iptables -t raw -D PREROUTING -j NOTRACK >/dev/null 2>&1
```

Upcoming builds with newer iptables should use:

```
iptables -t raw -D PREROUTING -j CT --notrack >/dev/null 2>&1
```


This router was setup via the GUI, Switch Config and Networking tab

- Trunk port on port 4 with tagged VLAN 1, VLAN 3 and VLAN 4
- As the GUI only supports tagging on all ports VLAN 1 is tagged, in this case it is no problem as long as the other side of the trunk port on the Main router VLAN1 is also tagged
- Port 2 added to VLAN3
- Port 3 added to VLAN 4


- br1 created no IP address, as this is just bridging via trunk VLAN 3 to br1 (192.168.53.1) of Main, so an IP address of 192.168.53.x is possible and can even be desirable if you want to reach the GUI on that address after we have enabled isolation on the Main router, however when you use this for IoT you actually do not want the router to be manageable from this subnet.
- br2 created no IP address, as this is just bridging via trunk VLAN 3 to br2 (192.168.54.1) of Main, so an IP address of 192.168.54.x is possible and can even be desirable if you want to reach the GUI on that address after we have enabled isolation on the Main router, however when you use this for IoT you actually do not want the router to be manageable from this subnet.
- VLAN 3 added to br1
- VLAN 4 added to br2
- VAP wl0.1 added to br1

Screenshots of WAP setup

WAN Connection Type


Connection Type Disabled 


Optional Settings

Router Name R7000 

Hostname

Domain Name

MTU Auto  1500

Shortcut Forwarding Engine Disable 

STP ☐ Enable ☒ Disable

Network Setup


Router IP

Local IP Address 192 168 5 7 / 24

Gateway 192 168 5 1

Local DNS 192 168 5 1

Dynamic Host Configuration Protocol (DHCP)

DHCP Type DHCP Server 

DHCP Server ☐ Enable ☒ Disable

Start IP Address 192 168 1 64

Maximum DHCP Users 190

Lease Expiration 1440 min

Static DNS 1 0 0 0 0

Static DNS 2 0 0 0 0

Static DNS 3 0 0 0 0

WINS 0 0 0 0

Use dnsmasq for DNS ☒

DHCP-Authoritative ☒

Default setup:

Virtual Local Area Network (VLAN)

VLAN Configuration

Vlans

☒ Enable
 ☐ Disable

VLAN Configuration	Port						Action
	CPUPORT	WAN	1	2	3	4	
	1000	1000	down	down	down	down	
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
							+
Tagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Autonegotiation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Gigabit		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Full Speed		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Full Duplex		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Enabled		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Save

Apply Settings

Cancel Changes

Trunk port 4 with VLAN 1, 3 and 4:

Virtual Local Area Network (VLAN)

VLAN Configuration

Vlans

☒ Enable
 ☐ Disable

VLAN Configuration	Port						Action
	CPUPORT	WAN	1	2	3	4	
	1000	down	down	down	down	down	
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-
							+
Tagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Autonegotiation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Gigabit		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Full Speed		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Full Duplex		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Enabled		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Save

Apply Settings

Cancel Changes

Tagging

Interface	Tag Number	Prio	Action
Add			

Bridging

Create a Bridge

Name	STP	IGMP Snooping	Prio	Forward Delay	Max Age	MTU	Root MAC	Action
br0	Off ▾	Off ▾	32768 ▾	15	20	1500	2C:30:33:53:5A:91 ⓘ	⊖
br1	STP ▾	Off ▾	32768 ▾	15	20	1500	2C:30:33:53:5A:91	⊖
br2	STP ▾	Off ▾	32768 ▾	15	20	1500	2C:30:33:53:5A:91	⊖
Add								

Assign to Bridge

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	Action
br1 ▾	vlan3 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖
br2 ▾	vlan4 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖
br1 ▾	wl0.1 ▾	On ▾	128 ▾	100	<input type="checkbox"/>	⊖
Add						

Current Bridging Table

Bridge Name	STP	Interface
br0	no	eth1 eth2 vlan1 vlan2
br1	yes	vlan3 wl0.1
br2	yes	vlan4

Network Configuration eth1

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration eth2

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration vlan1

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration vlan2

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration vlan3

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration vlan4

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration wl0.1

MAC Address

Label

TX Queue Length

Multicast to Unicast ☐ Enable ☒ Disable

Bridge Assignment ☒ Default ☐ Unbridged

Network Configuration br1

Label

TX Queue Length

MTU

Multicast Forwarding ☐ Enable ☒ Disable

Masquerade / NAT ☒ Enable ☐ Disable

Filter WAN NAT Redirection ☐ Enable ☒ Disable

Net Isolation ☐ Enable ☒ Disable

Forced DNS Redirection ☐ Enable ☒ Disable

IP Address /

L2Mesh Enable ☐

L2Mesh Bridge

Network Configuration br2

Label

TX Queue Length

1000

MTU

1500

Multicast Forwarding

Enable

Disable

Masquerade / NAT

Enable

Disable

Filter WAN NAT Redirection

Enable

Disable

Net Isolation

Enable

Disable

Forced DNS Redirection

Enable

Disable

IP Address

0

0

0

0

/

0

L2Mesh Enable

L2Mesh Bridge

br0

DHCPD

Multiple DHCP Servers

IP Address	Interface	Enable	Start	Max	Lease time
Add					

Save

Apply Settings

Cancel Changes

Isolating subnets/bridges

Theoretically VLANs are separated at the switch level but in the end they all come together at the main router.

Main router R7800

So isolation should be set at the Main router (R7800)

DDWRT bridges are by default FORWARDING to each other so there is no isolation at all and you should be able to freely connect to all subnets

To isolate bridges from each other, DDWRT has a GUI option on all interfaces: "Net isolation" this should be enabled to isolate the bridges (br1 and br2) from br0 and from the Main router (there is a bug in builds before 49732 which prevents to isolate a bridge from the router)

However bridges are not isolated from each other (patch is pending), so that has to be done manually by adding the following rules to the firewall:

```
## isolate bridges from each other:
iptables -D FORWARD -i br1 -o br+ -m state --state NEW -j REJECT
iptables -D FORWARD -i br2 -o br+ -m state --state NEW -j REJECT
iptables -I FORWARD -i br1 -o br+ -m state --state NEW -j REJECT
iptables -I FORWARD -i br2 -o br+ -m state --state NEW -j REJECT
```

Add to Administration > Commands and Save as Firewall

Although these rules are set at the Main router, this also applies to the WAP br1 and br2 because those are just an extension of the Main.

To put it differently the whole br1 and br2 network including the part which runs on the WAP should be isolated from br0 and the router(s)

It is possible that you have to further isolate br1 and br2 from the main router itself if you have a build before build 49732:

```
PORT_DHCP="67"
PORT_DNS="53"

# limit guests to essential router services (icmp, dns, dhcp)
for GUEST_IF in br1 br2
do
iptables -I INPUT -i $GUEST_IF -j REJECT
iptables -I INPUT -p icmp -i $GUEST_IF -j ACCEPT
iptables -I INPUT -p udp -i $GUEST_IF --dport $PORT_DHCP -j ACCEPT
iptables -I INPUT -p tcp -i $GUEST_IF --dport $PORT_DNS -j ACCEPT
iptables -I INPUT -p udp -i $GUEST_IF --dport $PORT_DNS -j ACCEPT
done
```

This part is not tested but is hopefully enough for a complete isolation,

To research

Is STP on the bridges necessary? Probably not as they are on different subnets

